Resumo de solução

Como se proteger contra programas potencialmente indesejados

Os programas potencialmente indesejados (PUPs) são discutidos em detalhes no **Relatório do McAfee Labs® sobre ameaças: fevereiro de 2015**. Qualquer aplicativo que o usuário possa achar benéfico, mas que apresente um risco oculto concreto para o usuário pode ser considerado um PUP. Os aplicativos geralmente não informam os usuários sobre esses riscos. Diferentemente de cavalos de Troia, vírus, rootkits e outras formas de malware, os PUPs não costumam garimpar credenciais do usuário (credenciais de mídias sociais, bancos e outras), nem alterar arquivos do sistema de maneira maliciosa. Os PUPs situam-se em uma zona intermediária de classificação porque frequentemente oferecem alguma vantagem ao usuário, além de serem um risco. Eles costumam ser difíceis de detectar e de categorizar.

Eis alguns dos comportamentos típicos dos PUPs:

- Modificar parâmetros de sistema, como as configurações do navegador, sem autorização.
- Ocultar um programa indesejado dentro de um aplicativo legítimo.
- Coletar sub-repticiamente informações do usuário, hábitos de navegação e configurações do sistema.
- Ocultar a instalação do aplicativo.
- Dificultar a remoção.
- Ser distribuído por meio de anúncios confusos e enganosos.

Os PUPs podem assumir uma variedade de formas:

- **Adware**: exibe anúncios, principalmente através de navegadores.
- **Descobridor/revelador de senhas**: mostra a senha oculta de um aplicativo.
- **Ferramenta de administração remota**: monitora as atividades do usuário na máquina na qual está instalado ou permite que o sistema seja controlado remotamente, sem conhecimento ou consentimento do usuário.
- **Keygen (gerador de chaves)**: gera chaves de produto de aplicativos legítimos.

intel Security

- **Sequestrador de navegador**: altera a página inicial, a página de pesquisa, configurações do navegador, etc.
- **Ferramentas de hacker**: aplicativos independentes que podem facilitar intrusões no sistema ou a perda de dados críticos.
- **Proxy**: redireciona ou oculta informações relacionadas a IP.
- **Ferramentas de rastreamento:** aplicativos de spyware ou keylogging que coletam pressionamentos de teclas do usuário, registram comunicações pessoais, monitoram as atividades on-line do usuário ou capturam telas sem o conhecimento do usuário.

Veja a seguir as principais diferenças entre PUPs e outros tipos de malware, como cavalos de Troia, ransomware, bots e vírus:

Técnicas	Programas potencialmente indesejados	Outros tipos de malware: cavalos de Troia, vírus e bots
Método de instalação	Procedimento padrão de instalação de aplicativos, às vezes com contrato de licença. Frequentemente exigem interação e anuência do usuário para serem completamente instalados em um sistema.	Instalados como um programa independente, sem qualquer interação com o usuário. Operam principalmente como um arquivo independente.
Apresentação	Agregados a aplicativos "limpos" e instalados de forma oculta juntamente com estes.	Arquivos independentes com alguns componentes adicionais. Não acondicionados como instaladores.
Desinstalação	Às vezes o pacote contém um desinstalador que permite a remoção. Frequentemente o processo de desinstalação é difícil.	Executáveis tornam mais complexa a remoção do malware devido a interceptações de outros processos, interceptações de identificadores de processos e outras ligações complexas. Como não são pacotes de instalador, não aparecem no Painel de controle.
Comportamento	Exibem anúncios, pop-ups e pop-unders indesejados Modificam configurações do navegador, coletam dados do sistema e do usuário ou permitem que o sistema seja controlado remotamente, sem conhecimento ou consentimento do usuário.	Roubam informações bancárias e de identificação pessoal, modificam arquivos do sistema, inviabilizam o uso do sistema, exigem resgate, etc.
Ocultação	Seu comportamento normalmente não é oculto.	Podem ocultar arquivos, pastas, entradas do Registro e tráfego de rede.

Entre todas as categorias de PUPs, o adware é a que mais chamou a atenção dos fornecedores de segurança — não devido aos anúncios incômodos, mas à forma como o adware abusa da confiança. O adware tornou-se mais inteligente com a implementação de várias técnicas para assegurar sua presença contínua nos sistemas infectados. Eis alguns dos métodos:

- Processo independente executado em memória.
- Arquivos DLL COM (Component Object Model) e não COM com funções criadas especificamente para o aplicativo.
- Chaves do Registro correspondentes a objetos auxiliares do navegador.
- DLLs que interceptam processos do sistema.
- Extensões e plug-ins de navegador.
- Serviços de sistema registrados.
- Componentes de drivers de dispositivos desempenhando funções de controle de dispositivos.
- Drivers de filtro de baixo nível.
- Cavalos de Troia entregues como carga.

Os PUPs costumam se propagar por meio de abuso da confiança de usuários inocentes, conforme explicado no **Relatório do McAfee Labs® sobre ameaças: novembro de 2014**. As técnicas de distribuição de PUPs mais comuns são:

- Anexação sub-reptícia a um aplicativo legítimo.
- Engenharia social.
- Venda de "curtir" do Facebook.
- Postagem de mensagens fraudulentas no Facebook.
- Sequestro do Google AdSense.
- Extensões e plug-ins de navegador indesejados.
- Instalação forçada, juntamente com aplicativos legítimos.

Como a Intel Security pode ajudá-lo a se proteger contra PUPs

McAfee Application Control

O **McAfee Application Control** permite que a sua empresa controle quais aplicativos têm permissão para serem executados no seu ambiente através de listas brancas dinâmicas e imposição de políticas para endpoints conectados e desconectados. Ele pode ajudar a proteger a sua empresa contra PUPs.

- **Listas brancas dinâmicas**: permitem que sua organização gerencie de forma eficiente os aplicativos relacionados em listas brancas, elaborando tais listas automaticamente conforme os sistemas são corrigidos e atualizados. O McAfee Application Control reduz a sua exposição a PUPs não permitindo a execução de adware conhecido.
- **Reputação de arquivos**: a integração com o **McAfee Global Threat Intelligence** (McAfee GTI) permite que o McAfee Application Control consulte canais de informação em tempo real sobre tipos de arquivos válidos conhecidos, inválidos e desconhecidos, contribuindo para a atualização das listas brancas e ajudando sua empresa a ficar ciente de aplicativos conhecidos como PUPs.
- **Mantenha-se protegido, conectado ou desconectado**: imponha controles a servidores conectados ou desconectados, máquinas virtuais, endpoints e dispositivos fixos, como terminais de ponto de venda.

McAfee Web Gateway

Anúncios enganosos, downloads de passagem e URLs maliciosos incorporados em sites confiáveis são apenas alguns dos métodos de ataque utilizados para fornecer PUPs. O **McAfee Web Gateway** é um produto sólido que reforça a proteção da sua empresa contra esse tipo de ameaça.

- **McAfee Gateway Anti-Malware Engine**: a análise de intenção sem assinaturas filtra o conteúdo malicioso do tráfego da Web em tempo real. O McAfee Gateway Anti-Malware Engine inspeciona os arquivos e impede que os usuários façam download caso tais arquivos sejam maliciosos.
- **Integração com o McAfee GTI**: os canais de categorização na Web, reputação na Web e a reputação de arquivos em tempo real do McAfee GTI oferecem proteção contra as ameaças mais recentes, pois o McAfee Web Gateway impede tentativas de conexão a sites maliciosos conhecidos ou a sites que usam redes de anúncios maliciosos.

McAfee Global Threat Intelligence
O **McAfee Global Threat Intelligence** (McAfee GTI) é um serviço abrangente de inteligência sobre ameaças em tempo real com base na nuvem que permite aos produtos da McAfee bloquear ameaças cibernéticas em todos os vetores — arquivos, Web, mensagens e rede. Garanta proteção proativa contra PUPs com os recursos abaixo:

- **Inteligência através da correlação de vetores**: coleta e correlaciona dados de todos os principais vetores de ameaças, incluindo arquivos, Web, e-mail e rede, para detectar ameaças mistas, como redes de anúncios que entregam malware assinado.
- **Plataforma de inteligência abrangente sobre ameaças**: coleta informações sobre ameaças de milhões de sensores em produtos McAfee distribuídos por clientes, como sistemas de prevenção de intrusões de rede, e-mail, Web e endpoint, além de dispositivos firewall.
- **Reputação de certificados**: consulta canais em tempo real de certificados válidos e inválidos para proteger sua empresa contra ameaças, como o malware assinado, que podem ser distribuídas por redes de anúncios maliciosos.
- **Security Connected**: integrada com outros produtos de segurança da McAfee para proporcionar os dados mais amplos sobre ameaças, a mais minuciosa correlação de dados e a mais completa integração de produtos disponível no momento, para garantir proteção contra adware.

McAfee SiteAdvisor® Enterprise
É desafiador manter-se um passo à frente do cenário de ameaças em constante mudança, principalmente quando tentamos proteger os usuários on-line contra ameaças, como os PUPs, sem impor políticas rígidas que comprometam a experiência do usuário.

- **Fácil identificação de ameaças, como sites maliciosos que se passam por sites legítimos**: com um sistema de classificação baseado em um intuitivo código de cores, o **McAfee SiteAdvisor Enterprise** oferece uma camada extra de proteção no desktop. Ele impede conexões com sites maliciosos conhecidos e informa os usuários sobre o perigo.
- **Segurança aprimorada oferecida pelo McAfee GTI**: o McAfee GTI oferece informações de inteligência sobre ameaças em tempo real para o McAfee SiteAdvisor Enterprise, o qual avalia os sites com base nas informações mais recentes.

McAfee Threat Intelligence Exchange
É imprescindível dispor de uma plataforma de inteligência capaz de se adaptar com o passar do tempo para atender às necessidades do seu ambiente. O **McAfee Threat Intelligence Exchange** reduz significativamente a exposição a ataques, graças à sua visibilidade sobre ameaças imediatas, como aplicativos ou arquivos desconhecidos em execução no ambiente.

- **Inteligência abrangente sobre ameaças**: personalize facilmente informações abrangentes sobre ameaças obtidas de fontes de dados de inteligência global. Essas fontes podem ser o McAfee GTI ou canais de terceiros, com informações locais sobre ameaças obtidas de dados de eventos históricos e em tempo real fornecidos via endpoints, gateways e outros componentes de segurança.
- **Prevenção de execução e correção**: o McAfee Threat Intelligence Exchange pode intervir e impedir que aplicativos desconhecidos sejam executados no ambiente. Caso um aplicativo cuja execução tenha sido permitida seja posteriormente considerado

malicioso, o McAfee Threat Intelligence Exchange pode desativar os processos em execução associados ao aplicativo em todo o ambiente, graças às suas poderosas capacidades de imposição de políticas e gerenciamento central.

- **Reputação de certificados**: a integração com o McAfee GTI protege a sua empresa em tempo real contra ataques que aproveitam o código malicioso assinado ao consultar canais em tempo real de certificados válidos e inválidos conhecidos. O McAfee Threat Intelligence Exchange pode proteger seus endpoints contra certificados maliciosos através de políticas gerenciadas de maneira centralizada, que podem ser implementadas para proteger endpoints tanto conectados quanto desconectados.

McAfee VirusScan® Enterprise

A detecção e limpeza de malware, incluindo adware, é simples com o **McAfee VirusScan Enterprise**. O McAfee VirusScan Enterprise utiliza o premiado mecanismo de varredura da McAfee para proteger os seus sistemas contra vírus, worms, rootkits, cavalos de Troia e outras ameaças avançadas.

- **Proteção proativa contra ataques**: integra tecnologia antimalware com prevenção de intrusões para proteção contra explorações que utilizam explorações de estouro de buffer direcionadas contra vulnerabilidades em aplicativos.
- **Detecção e limpeza de malware imbatíveis**: protege contra ameaças, como rootkits e cavalos de Troia, com análise comportamental avançada. Detém o malware utilizando técnicas como bloqueio de portas, nomes de arquivos, pastas/diretórios e compartilhamentos de arquivos, bem como rastreamento e bloqueio de infecções.
- **Segurança em tempo real com integração com o McAfee GTI**: proteção contra ameaças conhecidas e emergentes em todos os vetores de ameaças — arquivos, Web, e-mail e rede — com o suporte da plataforma de inteligência sobre ameaças mais abrangente do mercado.

Proteger a sua empresa contra PUPs que buscam contornar o modelo de confiança tradicional com comportamentos indesejados e traiçoeiros pode ser um desafio. A combinação da liderança em pesquisa do McAfee Labs com a tecnologia da Intel Security pode ajudar a sua empresa a se proteger contra PUPs.

McAfee. Part of Intel Security.
Av. das Nações Unidas, 8.501 - 16° andar
CEP 05425-070 - São Paulo - SP - Brasil
Telefone: +55 (11) 3711-8200
Fax: +55 (11) 3711-8286
www.intelsecurity.com